Product Guide

Management of Native Encryption 1.0

For use with ePolicy Orchestrator 4.6.6, 5.0.0, 5.0.1 Software

COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **5**

About this guide 5

Audience 5

Conventions 5

Find product documentation 6

1 Introduction **7**

Product components 7

Features 8

2 Installing MNE **9**

Overview of the installation process 9

Requirements 10

Installing the product 10

Deploy McAfee Agent for Mac through SSH 11

Install the MNE and Help extensions 11

Check in the MNE software packages 12

Deploy MNE to client systems 12

Send an agent wake-up call 13

Turn on FileVault on the client system 13

Uninstalling the product 14

Turn off FileVault 14

Remove MNE from the client system 15

Remove MNE and Help extensions 16

Remove the MNE software package 16

Manually uninstall MNE from the client system 17

Migrating from EEMac to MNE 17

Reporting FIPS status to client systems 17

3 Managing policies **19**

Product policies 20

Create a policy 21

Edit a policy 21

Assign a policy to a system 22

Assign a policy to a group 22

Enforce MNE policies on a system 23

Enforce policies to a group 23

4 Managing client systems **25**

Add a system to an existing group 25

Move systems between groups 26

System actions 26

How to run the MER tool 27

5 Managing MNE reports **29**

Queries as dashboard monitors 29
View the standard MNE reports 29
Create MNE custom queries 30
View the standard MNE dashboard 31
Create custom MNE dashboard 31
MNE client events 32

6 Recovering systems 35
Import the recovery key 35
Import the recovery key using System Tree 35
Import the recovery key using Data Protection 36
Perform system recovery 36
Provide the recovery key to the user 36
FileVault recovery key through scripting 37

Index 39

Preface

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

McAfee® Management of Native Encryption (MNE) is a management product that allows McAfee® ePolicy Orchestrator® (McAfee ePO™) administrators to manage Apple FileVault, which is an encryption product from Apple that provides encryption on Macintosh (Mac) systems.

McAfee Management of Native Encryption provides an easy-to-use administrative interface to perform these functions:

- Manage FileVault
- Report encryption status
- Recover systems

You can also use the reporting feature of MNE, without having to enable or disable FileVault, or manage FileVault policy.

We provide support only for MNE and not FileVault. If you encounter any issues on FileVault, we recommend that you contact Apple Support.

Contents

- *Product components*
- *Features*

Product components

MNE contains components and features that play a part in protecting your systems.

MNE

MNE integrates with the McAfee ePO server to enable or disable the FileVault disk encryption product on a Mac client system, as well as reporting FileVault status and managing FileVault policies.

McAfee ePO server

The McAfee ePO server provides a scalable platform for centralized policy management and enforcement of your security products and systems where they reside. MNE is integrated with the McAfee ePO console, where you can manage FileVault encrypted Mac client systems and deploy and manage the MNE product. The console provides comprehensive reporting and product deployment capabilities, all through a single point of control.

Product extensions and packages

The MNE extension that is installed on McAfee ePO allows managing and reporting of FileVault on Mac systems by deploying policy to client systems. The MNE software package that is checked in to the master repository on the McAfee ePO server is the actual product that is installed on the client system, and applies the policy received from McAfee ePO.

Features

You can manage FileVault through MNE using these features.

- **Management of FileVault** — FileVault can be enabled or disabled on client systems.
- **Password policy enforcement** — Enabling this option allows you to apply password settings on client systems.
- **Reporting** — FileVault status can be monitored on client systems.
- **System recovery** — FileVault recovery keys are escrowed in the McAfee ePO database, and might be retrieved through MNE to assist in recovery using Apple FileVault recovery tools.

We don't provide support for FileVault user management. However, if you still want to manage users, you must use the standard Apple controls that require administrative privileges.

2 Installing MNE

You need to perform a set of tasks to complete the installation process on the required client systems and manage them using McAfee ePO.

Contents

- *Overview of the installation process*
- *Requirements*
- *Installing the product*
- *Uninstalling the product*
- *Migrating from EEMac to MNE*
- *Reporting FIPS status to client systems*

Overview of the installation process

The installation and deployment process consists of these tasks.

This assumes that the user has already installed McAfee ePO on the client system. For more information about installing McAfee ePO, see the product documentation for your version of McAfee ePO.

1 Deploy McAfee® Agent for Mac to the client systems from McAfee ePO.

   A successful communication is established between the McAfee ePO server and McAfee Agent for Mac on the client systems.

2 Install the `MNEADMIN_1.0.0.x.zip` and `help_MNE_100.zip` extensions to the McAfee ePO server.

3 Check in the `MNE-1.0.0.x.zip` software package to the McAfee ePO server.

4 Deploy the software package to the required client system.

5 Send an agent wake-up call.

6 Turn on the **Turn On (Enable) FileVault** policy in McAfee ePO and enforce on the client system. You can also enable other policy options, as required. For more information, see the *Product policies* section.

   The client system prompts for a restart.

7 The user must restart the client system and type the password to authenticate.

   FileVault is enabled on the client system, and the user will now see the status **FileVault: Enabled** on the user interface.

Requirements

Make sure that your client systems meet these requirements before you install and deploy MNE.

Table 2-1 System requirements

Systems	Requirements
McAfee ePO server systems	See the product documentation for your version of McAfee ePO.
Client systems for MNE	• **CPU**: Works on all Intel-based Macs • **RAM**: 1 GB minimum • **Hard Disk**: 1 GB minimum free disk space

Table 2-2 Software requirements

Software	Requirements	
McAfee ePO	McAfee ePO 4.6.6, 5.0.0, and 5.0.1	
MNE	Extensions	• `MNEADMIN_1.0.0.x.zip` • `help_MNE_100.zip`
	MNE software package	• `MNE-1.0.0.x.zip`
McAfee Agent for Mac	McAfee Agent for Mac 4.8 or above	
Microsoft Windows Installer 3.0 Redistributable package (for McAfee ePO)	See the product documentation for your version of McAfee ePO.	
Microsoft .NET Framework 2.0 Redistributable package (for McAfee ePO)	See the product documentation for your version of McAfee ePO.	
Microsoft MSXML 6 (for McAfee ePO)	See the product documentation for your version of McAfee ePO.	

Table 2-3 Operating system requirements

Systems	Software
McAfee ePO server systems	See the product documentation for your version of McAfee ePO.
Client systems for MNE	• Mountain Lion: 10.8.2 and later (32- and 64-bit)

Installing the product

You need to install the MNE extensions and check in the software packages in to the master repository on the McAfee ePO server. A client deployment task is used to deploy the software package to client systems from the McAfee ePO server through the McAfee Agent for Mac, allowing these client systems to be managed by McAfee ePO.

Once the packages are deployed, the client system requires a restart to complete the installation. After the restart, the client communicates with the McAfee ePO server and manages FileVault according to the policies configured.

Deploy McAfee Agent for Mac through SSH

You can deploy McAfee Agent for Mac to client systems through Secure Shell (SSH).

Before you begin

To deploy McAfee Agent for Mac to your system, you must enable SSH (remote login). SSH can be enabled on your Mac system by enabling the **Remote Login** option under **System Preferences | Sharing | Remote Login**.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree** | **Actions** | **New Systems**.
3. Select the required option from **How to add systems**.
4. In the **Systems to add** field, type the NetBIOS name for each system, separated by commas, spaces, or line breaks. Alternatively, click **Browse** to select the systems.
5. Select **Push agents and add systems to the current group (My Organization)**.
6. In the **Target systems** field, add the IP address of the system where you want to deploy the McAfee Agent.
7. In the **Agent version** field, select **Non-Windows**, then select **McAfee Agent for Mac** from the drop-down list.
8. In the **Credentials for agent installation** field, enter administrator credentials of the Mac.
9. Click **OK** to trigger the McAfee Agent deployment on the Mac system.

To view the deployment status, click **Menu** | **Automation** | **Server Task Log**.

Install the MNE and Help extensions

Install the product and Help extensions to the McAfee ePO server.

The MNE extension contains the policy settings that can be enforced on to the required client systems and managed accordingly. The Help extension contains the Help content for the options in the user interface that appear when you click **?** in the user interface.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Software** | **Extensions**, then click **Install Extension** to open the **Install Extension** dialog box.
3. For each extension file, click **Browse**, select it, then click **OK**.

   You must install the extensions in this order:

   1. `MNEADMIN_1.0.0.x.zip`
   2. `help_MNE_100.zip`

   The **Install Extension** page displays the extension name and version.
4. Click **OK**.

Check in the MNE software packages

The software package must be checked in to the master repository so that you can use McAfee ePO to deploy the software to your client systems.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Software** | **Master Repository**, then click **Actions** | **Check In Package**.
3. From the **Package type** list, select **Product or Update (.zip)**, then browse and select the `MNE-1.0.0.x.zip` package file.
4. Click **Next** to open the **Package Options** page.
5. Click **Save**.

The new package appears in the **Packages in Master Repository** page under the respective branch in the repository.

Deploy MNE to client systems

Use this product deployment client task to deploy the product to your managed client systems.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Policy** | **Client Task Catalog**, select **McAfee Agent** | **Product Deployment** as **Client Task Types**, then click **Actions** | **New Task**.
3. Make sure that **Product Deployment** is selected, then click **OK**.
4. Type a name for the task you are creating and add any notes.
5. Next to **Target platforms**, select **Mac** to use the deployment.
6. Next to **Products and components**, set the following, then click **Save**:
   a. Select **McAfee Management of Native Encryption 1.0.0** to specify the version of the MNE package to be deployed.
   b. Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
7. Click **Menu** | **Systems** | **System Tree** | **Systems** tab, select the system where you want to deploy product, then click **Actions** | **Agent** | **Modify Tasks on a single system**.
8. Click **Actions** | **New Client Task Assignment** to open the **Client Task Assignment Builder** wizard.
9. On the **Select Task** page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select the task you created.

10 Next to **Tags**, select the required platforms that you are deploying the packages to, then click **Next**:
   - **Send this task to all computers**
   - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.

11 On the **Schedule** page, select whether the schedule is enabled, specify the schedule details, then click **Next**.

12 On the **Summary** page, review the summary, then click **Save**.

Send an agent wake-up call

The client system gets the policy update whenever it connects to the McAfee ePO server during the agent-server communication. However, you can force an immediate update with an agent wake-up call.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree**, then select a system or a group of systems from the left pane.

3 Select the **System Name(s)** of that group.

4 Click **Actions** | **Agent** | **Wake Up Agents**.

5 Select a **Wake-up call type** and a **Randomization** period (0-60 minutes) to define the length of time when all systems must respond to the wake-up call.

6 Under **Options**, select **Get full product properties**.

7 Under **Force policy update**, select **Force complete policy and task update**.

8 Click **OK**.

To view the status of the agent wake-up call, navigate to **Menu** | **Automation** | **Server Task Log**.

Turn on FileVault on the client system

You can turn on FileVault by enforcing the **Turn On (Enable) FileVault** policy on the client system.

Once the MNE software package is deployed to the client system, the MNE client integrates with the user interface of McAfee® Endpoint Protection for Mac 2.1 or McAfee® Virus Scan for Mac® 9.6, depending on what is already installed on that system. If neither product is available, the MNE deployment task installs the McAfee EPM 2.1 framework and MNE integrates into its user interface.

However, if the client system has McAfee EPM 2.0 or Virus Scan for Mac 9.5 already installed, the user must upgrade it to McAfee EPM 2.1 or Virus Scan for Mac 9.6 respectively, before installing MNE.

The user can see the status **FileVault: Disabled** on the user interface.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Policy** | **Policy Catalog**, select **McAfee Management of Native Encryption 1.0.0** from the **Product** drop-down list, then select **FileVault Product Settings** from the **Category** drop-down list.

3 Enable **Manage FileVault** | **Turn On (Enable) FileVault**.

You can also enable other policy options, as required. For more information, see the *Product policies* section.

4 Next to **Client Messaging**, enable the **Display the following message when enabling FileVault** option, and type a message that displays to the user after FileVault is enabled on the client system.

This step is optional.

5 Next to **Client Messaging**, enable the **Prompt for restart after FileVault is enabled** option, and type a message that displays to the user when the client system prompts for a restart.

This step is optional.

6 Click **Save**.

7 Click **Menu** | **Systems** | **System Tree** | **Systems** tab, then select the group in the System Tree where the system belongs. The list of systems belonging to this group appears in the details pane.

8 Select a system, then click **Actions** | **Agent** | **Modify Policies on a Single System**.

9 Select **McAfee Management of Native Encryption 1.0.0**, then click **Enforcing** next to **Enforcement status**.

10 Select **Break inheritance and assign the policy and settings below** to change the enforcement status.

11 Next to **Enforcement status**, select **Enforcing**, then click **Save**.

The client system prompts for a restart. The user must restart the system and enter the user's password to authenticate.

12 Send an agent wake-up call.

FileVault is turned on, and the user can now see the status **FileVault: Enabled** on the user interface.

Uninstalling the product

To uninstall MNE, you must perform these tasks.

- Turn off FileVault
- Remove MNE from McAfee ePO
- Remove MNE extensions and package
- Manually uninstall MNE from the client

Turn off FileVault

On the McAfee ePO console, you must modify the product setting policy to turn off FileVault. Make sure to note that you can turn off FileVault only if the client system is managed by McAfee ePO through MNE.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree** | **Systems**, then select a group under **System Tree**. All systems within this group (but not its subgroups) appear in the details pane.

3 Select a system, then click **Actions** | **Agent** | **Modify Policies on a Single System** to open the **Policy Assignment** page for that system.

4 From the **Product** drop-down list, select **McAfee Management of Native Encryption 1.0.0**. The policy **Categories** under MNE are listed with the system's assigned policy.

5 Select the **Product Setting** policy category, then click **Edit Assignments**.

6 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherit from**.

7 From the **Assigned policy** drop-down list, select a product setting policy.

From this location, you can edit the selected policy, or create a new policy.

8 Select whether to lock policy inheritance. Any system that inherit this policy can't have another one assigned in its place.

9 Enable **Manage FileVault** | **Turn Off (Disable) FileVault**.

10 Click **Save** on the **Policy Settings** page, then click **Save** on the **Product Settings** page.

11 Send an agent wake-up call.

On turning off the FileVault policy, all the encrypted drives get decrypted, and the status becomes **FileVault: Disabled**. This can take a few hours depending on the number and size of the encrypted drives.

Remove MNE from the client system

Use this product deployment client task to remove the software package from the client system.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Policy** | **Client Task Catalog**, select **McAfee Agent** | **Product Deployment** as Client Task Types, then click **Actions** | **New Task**.

3 Make sure that **Product Deployment** is selected, then click **OK**.

4 Type a name for the task and add any notes.

5 Next to **Target platforms**, select **Mac**.

6 Next to **Products and components** set the following:

a Select **McAfee Management of Native Encryption 1.0.0** to specify the version of the MNE package to be removed.

b Set the **Action** to **Remove**.

7 Click **Menu** | **Systems** | **System Tree** | **Systems** tab, select the system where you want to remove the product, then click **Actions** | **Agent** | **Modify Tasks on a single system**.

8 Click **Actions** | **New Client Task Assignment**.

9 On the **Select Task** page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select the task you created.

10 Next to **Tags**, select the desired platforms that you are removing the packages from, then click **Next**:
   - **Send this task to all computers**
   - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.

11 On the **Schedule** page, select whether the schedule is enabled, specify the schedule details, then click **Next**.

12 On the **Summary** page, review the summary, then click **Save**.

Remove MNE and Help extensions

You must remove MNE and the Help extensions from the McAfee ePO server to uninstall them from McAfee ePO.

You must remove the `MNEADMIN_1.0.0.x.zip` and `help_MNE_100.zip` extensions by following this procedure.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Software** | **Extensions**, then select **McAfee Management of Native Encryption 1.0.0**. The **Extension page** appears with the extension name and version details.

3 Click **Remove** on the required extension. The **Remove extension** confirmation page appears.

4 Click **OK** to remove the extension.

The MNE tables are not dropped from the database and must be manually dropped. This is to make sure that accidental removal of the MNE extension will not lose all the recovery keys.

Remove the MNE software package

When you turn off FileVault and remove the MNE software from the client system, you need to remove the MNE software package from the McAfee ePO server.

Before you begin

Make sure that you deactivate the MNE client before removing the MNE software package from McAfee ePO.

You need to remove the `MNE-1.0.0.x.zip` software package as follows.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Software** | **Master Repository**. The **Packages in Master Repository** page appears with the list of software packages and their details.

3 Click **Delete** next to the MNE software package.

4 Click **OK** to confirm.

Manually uninstall MNE from the client system

You can manually uninstall MNE from the client system, although McAfee ePO has all the required features for removing the product from the client system.

Before you begin

- You must have administrative privileges to perform this task.

Task

- From the command-line, type this command `sudo /usr/local/McAfee/uninstall MNE`. This removes the MNE software package from the client system.

Migrating from EEMac to MNE

You can migrate from EEMac to MNE by following these steps.

1. Check that the minimum version of McAfee Agent for Mac is 4.8 or above on the client system. If not, deploy McAfee Agent for Mac 4.8 or above. For more information, see the *Deploy McAfee Agent for Mac through SSH* topic.
2. Deploy MNE to the client system with the appropriate policy setting. For more information, see the *Deploy MNE to client systems* topic.
3. Deactivate and uninstall EEMac. For more information, see *McAfee Endpoint Encryption 7.0 Product Guide*.
4. Monitor the progress of EEMac in the dashboard to confirm that it is uninstalled. After EEMac is uninstalled, MNE will automatically enable FileVault at the next policy enforcement. For more information, see the *Enable FileVault on the client system* topic.

MNE will not enable FileVault on the client system if EEMac is installed and active.

Reporting FIPS status to client systems

The 140 series of Federal Information Processing Standards (FIPS) is a U.S. government computer security standards that specify requirements for cryptography modules.

MNE checks the client systems for FIPS certification and reports whether the client systems are running in FIPS mode or not. For this to happen, the user must perform these tasks.

1. Install the FIPS Administration tools. For more information about performing this task, see http://support.apple.com/kb/HT5396.
2. Send an agent wake-up call.

MNE will automatically report the FIPS status back to McAfee ePO.

For Mountain Lion 10.8.4 or above systems, the FIPS status is reported automatically to McAfee ePO by MNE, and the user does not have to install the FIPS Administration tools.

3 Managing policies

You can manage the MNE client systems from McAfee ePO through a combination of product policies. You assign policies to the required client systems to make sure that systems are managed and function as specified.

What is a policy?

A policy is a collection of settings that you create in McAfee ePO and assign it to the required MNE clients to make sure that client systems are configured and perform accordingly.

Are you configuring policies for the first time?

When configuring policies for the first time:

1. Plan product policies for different segments of your System Tree.
2. Create and assign policies to groups and systems.

Contents

- *Product policies*
- *Create a policy*
- *Edit a policy*
- *Assign a policy to a system*
- *Assign a policy to a group*
- *Enforce MNE policies on a system*
- *Enforce policies to a group*

Product policies

On the **Policy Catalog** page, the policies for the **Management of Native Encryption 1.0.0** product appear under the **FileVault Product Settings** category.

Table 3-1 Product policies

Settings	Description
FileVault Management	**Manage FileVault** — Allows you to manage FileVault and receive reports from the client system. • **Turn On (Enable) FileVault** — Allows you to turn on FileVault on client systems and manage accordingly. The client systems also report the status to McAfee ePO. • **Turn Off (Disable) FileVault** — Allows you to turn off FileVault on client systems. However, the client systems report the status to McAfee ePO. On enabling this option, the **Password Settings** function gets disabled. • **Destroy FileVault key when going to standby mode** — The FileVault recovery key will be removed from memory when a system goes into a standby mode. This defends against memory related attacks during various sleep states. Resuming from the sleep mode will force a user authentication to bring the key back into memory. **Do not manage FileVault** — FileVault cannot be managed and cannot receive FileVault information. You can only receive minimal system information. • **Report machine status** — Allows you to only receive reports from the client systems. FileVault cannot be managed and no changes can be made on the client system. You can report on BYOD (Bring Your Own Device) or contractor laptops to monitor compliance to company encryption policies. If FileVault is managed by MNE, the client system reports these to McAfee ePO: • FileVault status • FileVault mode • System information • System encryption status • FIPS status

Password Settings	**Enforce OS X User password requirements** — Allows you to set password settings on to OS X, which will enforce these password settings on the client system.
	If you disable this option, the **Password Settings** function gets disabled.
	• **Require at least one alphabetic character in password** — The user must include at least one alphabetic character in creating the password.
	• **Require at least one numeric character in password** — The user must include at least one numeric character in creating the password.
	  • **Minimum length __ (4-40)** — The user must create a password of the specified minimum length.
	  • **Maximum length __ (4-255)** — The user must create a password of the specified maximum length.
	• **Require change after the following number of days __ (1-180)** — The user must change the password after the specified number of days.

Client Messaging	**Prompt for restart after FileVault is enabled** — The user is notified to restart the client system when FileVault is enabled. The user is given 60 seconds warning about the restart and they can choose to cancel it. If they cancel it, FileVault changes will not be enforced until the system is restarted. Otherwise, the system will automatically attempt to restart after the 60 second period has expired.

Table 3-1 Product policies *(continued)*

Settings	Description
	Display the following message when enabling FileVault — The user receives a predefined message when FileVault is activated. **Display the following login banner** — The user sees a predefined login banner after authenticating into FileVault.

Create a policy

You can create policies from the Policy Catalog of McAfee ePO to assign them to required client systems to make sure that client systems are managed and function as specified. You can create policies before or after deploying MNE to the client systems.

By default, policies created here are not assigned to any groups or systems. When you create a policy, a custom policy is added to the Policy Catalog.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Policy** | **Policy Catalog**.
3. Click **Actions** | **New Policy**.
4. Select the policy **Category** from the drop-down list.
5. Select the policy that you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
6. Type a name for the new policy.
7. Type a description in the **Notes** field, if required, then click **OK**. The **Policy Settings** wizard opens.
8. Edit the policy settings on each tab, as required, then click **Save**.

Edit a policy

You can modify policies in the Policy Catalog and assign them to the required client systems, if required.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Policy** | **Policy Catalog**, then from the **Product** drop-down list, select **McAfee Management of Native Encryption 1.0.0**.
3. Select the policy **Category** from the drop-down list. All created policies for the selected category appear in the details pane.
4. Click the required policy, edit the required settings, then click **Save**.

Assign a policy to a system

You can assign a policy from the Policy Catalog to any system or system group. Assignment allows you to define policy settings once for a specific need, then apply that policy to multiple locations.

When you assign a new policy to a particular group, all child groups and systems that are set to inherit the policy from this assignment point, get the set policies.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**, then on the **Systems** tab under **System Tree**, select a group. All the systems within this group (but not its subgroups) appear in the details pane.
3. Select the target system, then click **Actions** | **Agent** | **Modify Policies on a Single System**. The Policy Assignment page for that system appears.
4. From the **Product** drop-down list, select **McAfee Management of Native Encryption 1.0.0**. The policy **Categories** under MNE are listed with the system's assigned policy.
5. Select the **Product Settings** policy category, then click **Edit Assignments**.
6. If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherit from**.
7. From the **Assigned policy** drop-down list, select the **Product Setting** policy.

   From this location, you can edit the selected policy or create a new policy.
8. Select whether to lock policy inheritance so that any systems that inherit this policy can't have another one assigned in its place.
9. Click **Save**.

Assign a policy to a group

You must assign policies to multiple managed systems within a group to make sure that client systems are managed and function as specified. You can assign policies before or after deploying MNE to the client systems.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree** | **Systems**, then select a group in the System Tree. All the systems within this group (but not its subgroups) appear in the details pane.
3. Select a system, then click **Actions** | **Agent** | **Set Policy & Inheritance** to open the **Assign Policies** page.
4. From the **Product** drop-down list, select **McAfee Management of Native Encryption 1.0.0**.
5. Select the **Category** and **Policy** from the drop-down lists, then click **Save**.

Enforce MNE policies on a system

Enable or disable policy enforcement on a client system. Policy enforcement is enabled by default, and is inherited in the System Tree.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree** | **Systems** tab, then under System Tree, select the group where the system belongs. The list of systems belonging to this group appears in the details pane.
3. Select a system, then click **Actions** | **Agent** | **Modify Policies on a Single System**.
4. Select **McAfee Management of Native Encryption 1.0.0**, then click **Enforcing** next to **Enforcement status**.
5. Select **Break inheritance and assign the policy and settings below** to change the enforcement status.
6. Next to **Enforcement status**, select **Enforcing**, then click **Save**.

After restarting, the client system communicates with the McAfee ePO server and pulls down the assigned MNE policies and encrypts the system according to the defined policies. The assigned user can be initialized through the Pre-Boot screen after the subsequent restart.

Enforce policies to a group

Enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree** | **Assigned Policies**, then select a group in the System Tree.
3. From the **Product** drop-down list, select **McAfee Management of Native Encryption 1.0.0**, then click **Enforcing** next to **Enforcement Status**.
4. To change the enforcement status, select **Break inheritance and assign the policy and settings below**.
5. Next to **Enforcement** status, select **Enforcing**.
6. Select whether to lock policy inheritance so that groups and systems that inherit this policy can't break enforcement, then click **Save**.

4 Managing client systems

System management allows you to import system information into McAfee ePO. This is useful in the process of installing MNE and viewing the list of FileVault users.

Client systems are managed by McAfee ePO through a combination of product policies. You can identify systems that require the same policy settings, and place them in a system group. This grouping allows you to update the policy settings to all systems in that group at the same time.

Contents

- *Add a system to an existing group*
- *Move systems between groups*
- *System actions*
- *How to run the MER tool*

Add a system to an existing group

You can import systems from your neighborhood network to groups through McAfee ePO. You can also import a network domain or Active Directory container.

The client systems are automatically added to the System Tree in McAfee ePO on successful installation of the McAfee Agent for Mac.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task

For option definitions, click **?** in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree**, then click **Actions** | **New Systems**.
3. From **How to add systems**, select the required option.
4. In the **Systems to add** field, type the NetBIOS name for each system, separated by commas, spaces, or line breaks. Alternatively, click **Browse** to select the systems.
5. Select **Push agents and add systems to the current group** to enable automatic **System Tree** sorting. Do this to apply the sorting criteria to these systems.

   Complete the following options:

Option	Action
Agent version	Select the agent version to deploy.
Installation path	Type the agent installation path or accept the default.

Option	Action
Credentials for agent installation	Type valid credentials to install the agent: • **Domain** — Type the domain of the system. • **User name** — Type the user name. • **Password** — Type the password.
Number of attempts	Type an integer for the specified number of attempts, or use zero for continuous attempts.
Retry interval	Type the interval in number of seconds between two attempts.
Abort After	Type the number of minutes before stopping the connection.
Connect using (McAfee ePO 4.6) or Push Agent using (McAfee ePO 4.6)	Select the connection used for the deployment: • **Selected Agent Handler** — Select the server from the list. • **All Agent Handlers**

6 Click **OK**.

Move systems between groups

You can move systems from one group to another in the System Tree. You can also move systems from any page that displays a table of systems, including the results of a query.

In addition to the steps below, you can also drag-and-drop systems from the Systems table to any group in the System Tree.

Even if you have a perfectly organized System Tree that mirrors your network hierarchy and uses automated tasks and tools to regularly synchronize your System Tree, you might need to move systems manually between groups. For instance, you might need to periodically move systems from the Lost&Found group.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree** | **Systems**, then browse and select the systems.

3 Click **Actions** | **Directory Management** | **Move Systems**.

4 Select whether to enable or disable, or to not change the System Tree sorting on the selected systems when they are moved.

5 Select the group where you want to place the systems, then click **OK**.

System actions

Use system actions to perform actions like FileVault recovery and import the recovery key.

You can perform these tasks by navigating through **Menu** | **Systems** | **System Tree**, select the required system, then click **Actions** | **Management of Native Encryption**.

Table 4-1 System actions

Option	Description
FileVault Recovery	You can recover a system, if a user reports accessibility issues to that system. To recover a system, select the required system in the System Tree, then click **Actions** | **Management of Native Encryption** | **FileVault Recovery** to open the recovery key for that system. You must send that recovery key to the user, so that the user can recover the system. For more information about recovering systems, see the *Recovering systems* section.
Import FileVault recovery key	You can manually import the recovery key of the client system to the McAfee ePO database using the **Import FileVault recovery key by Machine Node** page. For more information, see the *Recovering systems* section.

How to run the MER tool

The Minimum Escalation Requirements (MER) tool is used to collect diagnostic data for MNE and operating system details of the client system. You can run the MER tool in two ways.

How to run the MER tool on the Terminal application

You must run the MER tool on the Terminal application using the sudo privileges. After you authenticate, a diagnostic report log (`McAfeeMERTool_xxx.zip`) is created and located in your home directory.

```
sudo /usr/local//McAfee/MSCMertool -s McAfeeMERTool
```

How to run the MER tool using the McAfee EPM 2.1 interface

1 Open the McAfee Endpoint Protection for Mac 2.1 interface.

2 Navigate to **Help** | **Run MER Tool** to open the Terminal window.

3 Type the administrator password.

You see that a diagnostic report log (`McAfeeMERTool_xxx.zip`) is created under the user's home directory.

5 Managing MNE reports

MNE queries are configurable objects that retrieve and display data from the database. These queries can be displayed in charts and tables.

Any query results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitor.

Contents

- *Queries as dashboard monitors*
- *View the standard MNE reports*
- *Create MNE custom queries*
- *View the standard MNE dashboard*
- *Create custom MNE dashboard*
- *MNE client events*

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

MNE query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Reports are available in several formats:

- CSV — Use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Transform the data for other purposes.
- HTML — View the exported results as a web page.
- PDF — Print the results.

View the standard MNE reports

You can run and view the standard MNE reports from the **Queries & Reports** page.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Reporting** | **Queries & Reports**.

3 On the **Groups** pane, under the **Shared Groups** category, select **Management of Native Encryption**.

You can view these standard reports:

Query	Description
Report FileVault Status	Displays the FileVault status of the client systems.
Report overall encryption status of Mac systems	Displays the encryption status of the client systems.
Report Product Events	Displays the product related events for managing FileVault.
Report recovery keys	Displays the list of client systems with recovery information.
Reports users per machine	Displays the list of users assigned to a client system.

4 From the **Queries** list, select the required query.

5 Click **Actions** | **Run**. The query results appear.

You can also edit or duplicate the query, and view the details.

6 Click **Options** | **Export Data**, make the required selections, then click **Export** to export the query data.

7 Click on the .xml link to open the query data or right-click and save the .xml file to the required location.

8 Click **Close**.

Create MNE custom queries

You can create queries that retrieve and display the details like disk status, users, encryption provider, and product client events for MNE. With this wizard you can configure which data is retrieved and displayed, and how it is displayed.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Reporting** | **Queries & Reports**, then click **Actions** | **New**.

3 On the **Feature Group** pane, select **Management of Native Encryption**.

4 On the **Result Types** page, select the required query type, then click **Next**.

5 On the **Chart** page, from the **Display Result As** pane, select the type of chart or table to display the primary results of the query, then click **Next**.

If you select **Boolean Pie Chart**, you must configure the criteria to include in the query.

6 On the **Columns** page, from the **Available Columns** pane, select the columns to be included in the query, then click **Next**.

If you had selected **Table** on the **Chart** page, the columns you select here are the columns of that table. Otherwise, these are the columns that make up the query details table.

7 On the **Filter** page, from the **Available Properties** pane, select the required properties to narrow the search results, then click **Run**. The Unsaved Query page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.

Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property.

- If the query didn't appear to return the expected results, click **Edit Query** to go back to the Query Builder and edit the details of this query.
- If you don't need to save the query, click **Close**.
- If this is a query you want to use again, click **Save** and continue to the next step.

8 On the **Save Query** page, type a name for the query, add any notes, and select one of the following:

- **New Group** — Type the new group name and select either:
  - **Private (Private Groups)**
  - **Public (Shared Groups)**
- **Existing Group** — Select the group from the list of Shared Groups.

9 Click **Save**.

View the standard MNE dashboard

You can view the standard MNE reports from the **Dashboards** page.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Dashboard** drop-down list, select **MNE FileVault Dashboard**.

You can view the dashboard.

Create custom MNE dashboard

Dashboards are collections of user-selected and configured monitors that provide current data about your environment. You can create your own dashboards from query results or use McAfee ePO's default dashboards.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the **Dashboard** drop-down list, select **MNE FileVault Dashboard**.

3 From the **Dashboard Actions** drop-down list, select **New**.

4 Next to **Dashboard Name**, type a name for the dashboard.

5 Next to **Dashboard Visibility**, select one of these options, as required:

- **Private** — To make the dashboard visible to a specific set of users.
- **Public** — To make the dashboard visible to all the users.
- **Shared with the following permission set(s)** — To make the dashboard visible to the specified permission set(s).

6 Click **OK**.

MNE client events

While implementing and enforcing the MNE policies that control how sensitive data is encrypted, you can monitor real-time client events and generate reports using the MNE client events query.

Event ID	Event Description	Event Type
35203	This event is reported in McAfee ePO when the FileVault activation is failed with an error message "OS X recovery partition is not found".	Critical
35204	This event is reported in McAfee ePO when the product is found incompatible.	Informational
35205	This event is reported in McAfee ePO when FileVault activation is successful.	Informational
35206	This event is reported in McAfee ePO when the restart prompt appears on the client system.	Informational
35207	This event is reported in McAfee ePO when the FileVault activation is failed with an error message "Unsupported operating system found".	Critical
35208	This event is reported in McAfee ePO when FileVault activation is failed with an error message "EEMac is active".	Informational
35210	This event is reported in McAfee ePO when FileVault activation is failed with an error message "Unable to retrieve the recovery key from FileVault".	Error
35211	This event is reported in McAfee ePO when FileVault activation is failed with an error message "Unknown exception occurred".	Error
35212	This event is reported in McAfee ePO when the recovery key is sent to the McAfee ePO database successfully.	Informational
35213	This event is reported in McAfee ePO when the user is waiting for system to restart.	Informational
35214	This event is reported in McAfee ePO when MNE is running in Report and Manage mode.	Informational
35215	This event is reported in McAfee ePO when MNE is running in Report only mode.	Informational
35216	This event is reported in McAfee ePO when MNE is disabled.	High
35217	This event is reported in McAfee ePO when OS X login banner is applied.	Informational
35218	This event is reported in McAfee ePO when OS X login banner is removed.	Informational
35219	This event is reported in McAfee ePO when OS X password settings are applied.	Informational
35220	This event is reported in McAfee ePO when OS X password settings are disabled.	Critical

Event ID	Event Description	Event Type
35221	This event is reported in McAfee ePO when disabling FileVault is failed as the recovery key is unavailable, and the user must manually disable FileVault.	Error
35222	This event is reported in McAfee ePO when disabling FileVault is failed as the recovery key is invalid, and the user must manually disable FileVault.	Error
35223	This event is reported in McAfee ePO when the Mac serial number is not found.	Error
35224	This event is reported in McAfee ePO when the volume information is not available.	Error
35225	This event is reported in McAfee ePO when FIleVault user information is sent.	Informational
35226	This event is reported in McAfee ePO when FileVault is disabled by third party application or user.	Critical

6 Recovering systems

System recovery is a process of recovering a user's system from system crashes, system malfunctions, accessibility issues, and more. If a user reports any such problems, you must provide the recovery key of the system to the user for the user to recover the system using FileVault recovery tools that is provided by Apple.

We don't provide support for FileVault recovery tools. If you encounter any problems with this recovery process, we recommend that you contact Apple Support.

How to obtain the recovery key?

The recovery key can be obtained in two ways:

- When enabling FileVault on a client system using MNE, MNE obtains the recovery key of the system automatically and sends it to the McAfee ePO database.
- If FileVault has been previously enabled by the user at the point when MNE is installed on the client system, then you must import the recovery key of the system manually into the McAfee ePO database in order for the recovery feature to be available for that system.

You can obtain the recovery key of a client system only if FileVault is managed by MNE.

How to obtain the serial number of the Mac system?

The serial number of the Mac system can be obtained in two ways:

- At the back of your Mac hardware, the serial number of the system is displayed.
- When you click the **About this Mac** option, the serial number of the system is displayed.

Contents

- *Import the recovery key*
- *Perform system recovery*

Import the recovery key

You must manually import the recovery key of the client system to the McAfee ePO database using the **System Tree** or **Data Protection** menu. You must perform this task only if FileVault has been previously enabled by the user.

Import the recovery key using System Tree

You must manually import the recovery key of the client system to the McAfee ePO database using the **Import FileVault recovery key by Machine Node** page.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Systems** | **System Tree** | **Systems** tab, select the required system, then click **Actions** | **Management of Native Encryption** | **Import FileVault recovery key** to open the **Import FileVault recovery key by Machine Node** page.

3 In the **Enter recovery key** field, type the recovery key of the system that you obtained.

4 Click **Ok**.

Import the recovery key using Data Protection

You must manually import the recovery key of the client system to the McAfee ePO database using the **Import FileVault recovery key by serial number** page.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Data Protection** | **Import FileVault recovery key** to open the **Import FileVault recovery key by serial number** page.

3 In the **Enter serial number** field, type the serial number of the system that you received from the user.

4 In the **Enter recovery key** field, type the recovery key of the system that you obtained.

5 Click **Ok**.

Perform system recovery

If a user reports the system to be recovered, you must provide the recovery key of the system to the user for the user to recover the system using the Apple FileVault recovery tools.

Provide the recovery key to the user

You must provide the recovery key of the client system that is managed by McAfee ePO to the user for the user to recover the system using the Apple FileVault recovery tools.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Data Protection** | **FileVault recovery**.

You can also access **FileVault recovery** by navigating through **Menu** | **Systems** | **System Tree** | **Systems** tab, select the required system, then click **Actions** | **FileVault recovery**.

3 On the **Enter serial number** page, type the **Serial number** of the system that you received from the user, then click **Next**.

This step is not applicable if you access **FileVault recovery** through the **System Tree** menu, because the serial number of the system is automatically populated.

The recovery key of the system appears on the **Response code from serial number** page.

4 Provide the recovery key to the user so that the user can recover the system.

Once the user has received the recovery key, we recommend the user to contact Apple Support for recovering the client system.

FileVault recovery key through scripting

FileVault recovery key can be retrieved from McAfee ePO using scripting by passing serial number or McAfee ePO leaf node.

How does scripting work?

Scripts using the Web API can be run from any computer that can connect to the ePolicy Orchestrator server. For security reasons, they should not be run on the same computer as the ePolicy Orchestrator server itself.

The Web API is used primarily for two purposes:

- Scripting sequences of tasks
- Performing simple tasks without using the user interface

FileVault key recovery by serial number

FileVault recovery key can be retrieved from McAfee ePO using the `mc.mne.recoverMachine` command by passing the serial number of the system.

Command	Syntax	Description

mc.mne.recoverMachine	`mc.mne.recoverMachine(serialNumber='< >')`
	For example,
	`mc.mne.recoverMachine(serialNumber='12345')`
		Pass the serial number of the client system to retrieve the FileVault recover key.

FileVault key recovery by McAfee ePO leaf node

FileVault recovery key can be retrieved from McAfee ePO using `mc.mne.recoverMachine` command by passing the McAfee ePO leaf node id number.

Command	Syntax	Description

mc.mne.recoverMachine	`mc.mne.recoverMachine(epoLeafNodeId='<>'`
	For example,
	`mc.mne.recoverMachine(epoLeafNodeId='10')`
		Pass the McAfee ePO leaf node id to retrieve the FileVault recover key for the client system.

Index

A

about this guide 5
agent wake-up call, sending 13

C

client events, viewing 29
client systems
    actions 26
    adding and importing 25
    managing 25
    moving 26
    recovering 35, 36
client, MNE
    deactivating 14
    installing 9, 10
    migrating 17
    uninstalling 17
conventions and icons used in this guide 5

D

dashboards, MNE
    creating 31
    viewing 31
disk status
    reporting 29
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5

E

extensions, MNE
    installing 11
    removing 16
    uninstalling 14

F

features
    FileVault recovery 8
    management of FileVault 8
    password policy enforcement 8
    reporting 8

I

installation
    MNE extensions 11

M

McAfee Agent for Mac, downloading and deploying 11
McAfee ServicePortal, accessing 6
MER tool, using 27
MNE
    removing 14

P

packages, installing
    MNE 12
policies
    assigning to systems 22
    categories 20
    creating 21
    disabling 14
    editing 21
    enforcing 23
    managing 19
product components
    client system 7
    extensions 7
    McAfee ePO 7
    policies 7
    software packages 7
product setting policy
    disabling 14
product version, reporting 29

Q

queries, MNE
    creating 30
    dashboard monitor 29
    running 29

R

reports, MNE
    exporting results 29
    managing 29

reports, MNE *(continued)*
viewing 29
requirements, MNE 10

S

ServicePortal, finding product documentation 6
software package, MNE
removing 14–16
software packages, MNE
checking in 12
deploying 12

T

Technical Support, finding product information 6

U

users
reporting 29

V

volume status, reporting 29

McAfee
An Intel Company